IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A system for detecting intrusion on a host, comprising:
   a) a source of rules;
   b) a source of facts; and
   c) an analysis engine comprising a processor in communication with the source of rules and source of facts, configured to ~~apply~~ determine whether an intrusion has taken place by applying forward- and backward-chaining using facts from the source of facts and rules from the source of rules by:

      (i) using forward chaining to generate one or more inferences:

      (ii) determining which, if any, of the inferences matches a sub-goal associated with a rule from the source of rules;

      (iii) with respect to each inference that matches a sub-goal, applying backward chaining from that sub-goal's potential parents into other sub-goals; and

      (iv) for each sub-goal reached either by forward or backward chaining, determining whether the sub-goal indicates an intrusion has taken place.

2. (Original) The system as recited in claim 1, wherein the analysis engine performs forward-chaining by using the facts to generate inferences using the rules, and the analysis engine is further configured to limit lengths of the forward-chaining.

3. (Original) The system as recited in claim 2, wherein the analysis engine is configured to perform backward-chaining from a goal and produce at least one sub-goal.

4. (Canceled)

5. (Original) The system as recited in claim 3, wherein the analysis engine is configured to assign a score to the goal.

6. (Original) The system as recited in claim 4, wherein the score comprises at least one of a cost function, a confidence factor, a support value, and importance of the goal.

7. (Currently amended) The system as recited in claim 5, wherein the analysis engine is further configured to use continuations to schedule the processing of a goal based at least in part on whether the data required to continue processing the goal is available.

8. (Original) The system as recited in claim 7, wherein the analysis engine is further configured to use the scores to select a goal to be pursued.

9. (Original) The system as recited in claim 8, wherein the rules are configured to enable the system to detect an intrusion after occurrence of the intrusion.

10. (Original) The system as recited in claim 9, wherein the rules are configured to cause the analysis engine to correlate and evaluate facts from a plurality of sources of facts.

11. (Original) The system as recited in claim 10, wherein the plurality of sources comprises primary, secondary, and indirect sources of facts.

12. (Original) The system as recited in claim 10, wherein the rules are further configured to cause the analysis to collect, correlate, and evaluate facts related to all phases of an attack.

13. (Original) The system as recited in claim 2, wherein the analysis engine is configured to correlate and evaluate incomplete facts to detect attacks with missing or forged facts.

14. (Original) The system as recited in claim 1, further comprising a user interface, wherein the analysis engine is configured to provide the user interface with an analysis based on the facts and rules, and provide the user interface with information relating to the analysis.

15. (Original) The system as recited in claim 14, wherein the analysis engine is further configured to provide background information relating to the analysis.

16. (Currently amended) A method for detecting intrusions on a host, comprising the steps of:

a) providing a source of rules and a source of facts;

b) forward- and backward-chaining using facts from the source of facts and rules from the source of rules by:

(i) using forward chaining to generate one or more inferences:

(ii) determining which, if any, of the inferences matches a sub-goal associated with a rule from the source of rules;

(iii) with respect to each inference that matches a sub-goal, applying backward chaining from that sub-goal's potential parents into other sub-goals; and

(iv) for each sub-goal reached either by forward or backward chaining, determining whether the sub-goal indicates an intrusion has taken place.

17. (Currently amended) A computer program product for detecting intrusions on a host, the computer program product being embodied in a computer readable medium having machine readable code embodied therein for performing the steps of:

a) providing a source of rules and a source of facts;

b) forward- and backward-chaining using facts from the source of facts and rules from the source of rules by:

(i) using forward chaining to generate one or more inferences:

(ii) determining which, if any, of the inferences matches a sub-goal associated with a rule from the source of rules;

(iii) with respect to each inference that matches a sub-goal, applying backward chaining from that sub-goal's potential parents into other sub-goals; and

(iv) for each sub-goal reached either by forward or backward chaining, determining whether the sub-goal indicates an intrusion has taken place.